infected with the SubSeven Trojan. SubSeven is a Trojan Horse that can permit a remote computer to gain complete control of an infected machine, typically by using Internet Relay Chat (IRC) channels for communications. In June 1998 and February 1999, the Director of the Central Intelligence Agency testified before Congress that several nations recognize that cyber attacks against civilian computer systems represent the most viable option for leveling the playing field in an armed crisis against the United States. The Director also stated that several terrorist organizations believed information warfare to be a low cost opportunity to support their causes. We must, as a nation, prepare both our public and private sectors to protect ourselves against such efforts.

That is why I am again introducing legislation that gives critical infrastructure industries the assurances they need in order to confidently share information with the federal government. As we learned with the Y2K model, government and industry can work in partnership to produce the best outcome for the American people. Today, the private sector has established many information sharing organizations (ISOs) for the different sectors of our nation's critical infrastructure. Information regarding a cyber threat or vulnerability is now shared within some industries but it is not shared with the government and it is not shared across industries. The private sector stands ready to expand this model but have also expressed concerns about voluntarily sharing information with the government and the unintended consequences they could face for acting in good faith. Specifically, there has been concern that industry could potentially face antitrust violations for sharing information with other industry partners, have their shared information be subject to the Freedom of Information Act, or face potential liability concerns for information shared in good faith. My bill will address all three of these concerns. The Cyber Security Information Act also respects the privacy rights of consumers and critical infrastructure operators. Consumers and operators will have the confidence they need to know that information will be handled accurately, confidentially, and reliably.

The Cyber Security Information Act is closely modeled after the successful Year 2000 Information and Readiness Disclosure Act by providing a limited FOIA exemption, civil litigation protection for shared information, and an antitrust exemption for information shared among private sector companies for the purpose of correcting, avoiding, communicating or disclosing information about a cyber-security related problem. These three protections have been requested by the U.S. Chamber of Commerce, the National Association of Manufacturers, the Edison Electric Institute, the Information Technology Association of America, Americans for Computer Privacy, and the Electronics Industry Alliance. Many private sector companies have also asked for this important legislation. I have attached to my statement a letter from the many professional associations and private sector companies supporting the introduction of this measure.

This legislation will enable the private sector, including ISOs, to move forward without fear from the government so that government and industry may enjoy a mutually cooperative partnership. This will also allow us to get a timely and accurate assessment of the vulnerabilities of each sector to cyber attacks and allow for the formulation of proposals to eliminate these vulnerabilities without increasing government regulation, or expanding unfunded federal mandates on the private sector.

ISOs will continue their current leadership role in developing the necessary technical expertise to establish baseline statistics and patterns within the various infrastructures, as clearinghouses for information within and among the various sectors, and as repositories of valuable information that may be used by the private sector. As technology continues to rapidly improve industry efficiency and operations, so will the risks posed by vulnerabilities and threats to our infrastructure. We must create a framework that will allow our protective measures to adapt and be updated quickly.

It is my hope that we will be able to move forward quickly with this legislation and that Congress and the Administration will work in partnership to provide industry and government with the tools for meeting this challenge. A Congressional Research Service report on the ISOs proposal describes the information sharing model as one of the most crucial pieces for success in protecting our critical infrastructure, yet one of the hardest pieces to realize. With the introduction of the Cyber Security Information Act of 2001, we are removing the primary barrier to information sharing between government and industry. This is landmark legislation that will be replicated around the globe by other nations as they too try to address threats to their critical infrastructure.

Mr. Speaker, I believe that the Cyber Security Information Act of 2001 will help us address critical infrastructure cyber threats with the same level of success we achieved in addressing the Year 2000 problem. With government and industry cooperation, the seamless delivery of services and the protection of our nation's economy and well-being will continue without interruption just as the delivery of services continued on January 1, 2000.

JULY 5, 2001.

Hon. ——
U.S. House of Representatives,
Washington, DC

DEAR REPRESENTATIVE: We, the undersigned, representing every sector of the United States economy, write today to strongly urge you to become an original cosponsor of the Cyber Security Information Act to be shortly introduced by Representatives Tom Davis and Jim Moran. This important bill will strengthen information sharing legal protections that shield U.S. critical infrastructures from cyber and physical attacks and threats.

Over the past four years, industry-government information sharing regarding vulnerabilities and threats has been a key element of the federal government's critical infrastructure protection plans. Several industry established information sharing organizations, including Information Sharing and Analysis Centers (ISACs) and the Partnership for Critical Infrastructure Security (PCIS), have been set up to support this initiative. The National Plan for Information Systems Protection, version 1.0, also calls for private sector input about actions that will facilitate industry-government information sharing.

As representative companies and industry associations involved in supporting the ongoing development of a National Plan for critical infrastructure protection, we believe that Congress can play a key role in facilitating this initiative by passing legislation to support the Plan's strategic objectives.

Currently, there is uncertainty about whether existing law may expose companies and industries that voluntarily share sensitive information with the federal government to unintended and potentially harmful consequences. This uncertainty has a chilling effect on the growth of all information sharing organizations and the quality and quantity of information that they are able to gather and share with the federal government. As such, this situation is an impediment to the effectiveness of both industry and government security and assurance managers to understand, collaborate on and manage their vulnerability and threat environments.

Legislation that will clarify and strengthen existing Freedom of Information Act and antitrust exemptions, or otherwise create new means to promote critical infrastructure protection and assurance would be very helpful and have a catalytic effect on the initiatives that are currently under way.

Companies in the transportation, telecommunications, information technology, financial services, energy, water, power and gas, health and emergency services have a vital stake in the protection of infrastructure assets. With over 90 percent of the country's critical infrastructure owned and/or operated by the private sector, the government must support information sharing between the public and private sectors in order to ensure the best possible security for all our citizens. A basic precondition for this cooperation is a clear legal and public policy framework for action.

Businesses also need protection from unnecessary restrictions placed by federal and state antitrust laws on critical information sharing that would inhibit identification of R&D needs or the identification and mitigation of vulnerabilities. There are a number of precedents for this kind of collaboration, and we believe that legislation based on these precedents will also assist this process.

Faced with the prospect of unintended liabilities, we also believe that any assurances that Congress can provide to companies voluntarily collaborating with the government in risk management planning activity—such as performing risk assessments, testing infrastructure security, or sharing certain threat and vulnerability information—will be very beneficial. Establishing liability safeguards to encourage the sharing of threat and vulnerability information will add to the robustness of the partnership and the significance of the information shared.

Thank you for considering our views on this important subject. We think that such legislation will contribute to the success of the institutional, information-sharing, technological, and collaborative strategies outlined in Presidential Decision Directive—63 and version 1.0 of the National Plan for Information Systems Protection.

Sincerely,
Americans for Computer Privacy.
Edison Electric Institute.
Fannie Mae.
Internet Security Alliance.
Information Technology Association of America.
Microsoft.
National Center for Technology and Law, George Mason University.
Owest Communications.
Security.
Computer Sciences Corporation.
Electronic Industries Alliance.
The Financial Services Roundtable.
Internet Security Systems.
National Association of Manufacturers.
Mitretek Systems.
The Open Group.